



# UNITED STATES PATENT AND TRADEMARK OFFICE

*Arne*  
UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/679,541	10/06/2000	Kouya Tochikubo	198274US2TTC	8841
22850	7590	04/05/2005	EXAMINER	
OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C. 1940 DUKE STREET ALEXANDRIA, VA 22314			LANIER, BENJAMIN E	

DATE MAILED: 04/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>
	09/679,541	TOCHIKUBO ET AL.
	<b>Examiner</b> Benjamin E Lanier	<b>Art Unit</b> 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 03 March 2005.  
 2a) This action is FINAL.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1,4,6,7,9 and 14-39 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1,4,6,7,9 and 14-39 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 06 October 2000 is/are: a) accepted or b) objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
     1. Certified copies of the priority documents have been received.  
     2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
     3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date: _____
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date: _____	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____

## **DETAILED ACTION**

### ***Response to Amendment***

1. Applicant's argument filed 03 March 2005 amends claims 1, 4, 6, 7, 9, cancels claims 2, 3, 5, 8, 10-13, and adds claims 14-39. Applicant's amendment has been fully considered and is entered.

### ***Response to Arguments***

2. Applicant's arguments filed 03 March 2005 have been fully considered but they are not persuasive. Applicant's argument that Otsuki does not disclose an encryption algorithm management system including a terminal unit and a center unit that renew a common cipher-key when receiving encrypted data at the terminal unit or when receiving a demand at the center unit is not persuasive because Otsuki discloses that the software supplier and the user terminal contain a common key generator that generates a new common key for each software program that is requested by the user (Fig. 2, Col. 7, line 39 – Col. 8, line 3).

3. Applicant's argument that Otsuki does not disclose a means for the user to demand that encrypted data be received from the software supplier is not persuasive because Figures 2 and 3 show a communication means between the software supplier and the user and the user sends requests to the software supplier (Col. 2, lines 53-57).

4. Applicant's argument that Otsuki does not disclose that the software supplier and the user have a common cipher-key is not persuasive because Figures 2 and 3 clearly show the software supplier and the user having a common key.

5. Applicant's argument that Otsuki does not disclose that the common key is renewed so as to be identical with said renewed key in case of receiving said demand from said transmitter is

Art Unit: 2132

not persuasive because Otsuki discloses that the common is generated using the program identifier of the program requested by the user (Col. 7, line 39 – Col. 8, line 3), which would make the keys at the supplier and user identical.

6. Applicant's arguments the Otsuki does not teach the limitations of the new claims is not persuasive and are addressed below.

***Claim Rejections - 35 USC § 102***

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1, 4, 6, 7, 9, 14, 16-20, 22-25, 27-32, 34-38 are rejected under 35 U.S.C. 102(b) as being anticipated by Otsuki, U.S. Patent No. 5,751,805. Referring to claims 1, 4, 7, 24, 31, 37, Otsuki discloses a data protecting system wherein upon purchase of an encrypted software package a user requests his identifier and decryption key from the software house (Col. 4, lines 1-17), which meets the limitation of a transmitter configured to transmit a demand to said center unit for obtaining an encrypted data needed for decrypting said ciphered encryption algorithm. The software house distributes the random encryption key to the user encrypted with the identifier (Col. 4, lines 1-10), which meets the limitation of a key controller configured to renew said common cipher-key so as to be identical with said renewed common cipher-key in case of receiving said demand from said transmitter, and an encoder configured to produce said encrypted data by encrypting a cipher-key with said renewed common cipher-key and to transmit said encrypted data to said terminal unit. Once the user receives the encrypted random

Art Unit: 2132

encryption key the software installation module can prepare the loader to decrypt the software (Col. 4, lines 18-21). The encrypted random key is then decrypted using the identifier entered by the user. Once decrypted the random key is then used to decrypt an encrypted encryption algorithm that is stored on the user's IC card in order to decrypt the encrypted software (Col. 4, lines 34-46), which meets the limitation of an encryption controller configured to renew said common cipher-key in case of receiving said encrypted data from said center unit in response to said demand, and to produce an encryption algorithm by decrypting said encrypted data with the renewed common cipher-key.

Referring to claim 6, Otsuki discloses that the encryption information can be stored on a CD-ROM (Col. 6, lines 17-25).

Referring to claim 9, Otsuki discloses that the users are authenticated before their requests are granted (Abstract), which meets the limitation of a verification controller configured to verify whether said terminal unit is authorized to use said encryption algorithm at the time of receiving said demand from said terminal unit, and to have said key controller renew said common cipher-key only if said terminal unit has the authorization.

Referring to claims 14, 20, 25, 32, Otsuki discloses that the algorithm is supplied to the user terminal (Abstract), therefore the algorithm would be stored in a memory of that terminal once received.

Referring to claims 16, 17, 22, 23, 27, 28, 34, 35, Otsuki discloses that after decrypting the algorithm the user requests the encrypted software program (Col. 4, lines 12-17), which meets the limitation of transmitting a demand when the encryption algorithm is decrypted,

transmitting a demand every predetermined number of times that the encryption algorithm is decrypted.

Referring to claims 18, 29, 36, Otsuki discloses a common key generation section for generation the common key (Fig. 3), which meets the limitation of encryption controller is stored in a memory area that may not be read or rewritten by outsiders.

Referring to claims 19, 30, 38, Otsuki discloses that the user is authorized at the supplier using the user password/pin (Col. 5, lines 26-47), which meets the limitation of center unit further comprises a verification controller configured to determine if said terminal unit is authorized to use said encryption algorithm at the time of receiving said demand from said terminal unit, and to have said key controller renew said common cipher-key only if said terminal unit is determined to be authorized.

#### ***Claim Rejections - 35 USC § 103***

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Art Unit: 2132

11. Claims 15, 21, 26, 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Otsuki, U.S. Patent No. 5,751,805, in view of Ostermann, U.S. Patent No. 4,484,025. Referring to claims 15, 21, 26, 33, Otsuki discloses the distribution of ciphered encryption algorithms in a software environment, but not a communications environment. Ostermann discloses a system of enciphered communications between a first and second terminal (Fig. 1) wherein a control center stores a plurality of encryption algorithms that are sent to the terminals so that they may perform secure communications using the same algorithm (Col. 1, lines 46-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of distributing ciphered encryption algorithms of Otsuki for communication purposes because of the demand for enciphered communication exchanges and because having multiple encryption algorithms available to a plurality of communicating terminals provides the terminals with greater communication flexibility as taught by Ostermann (Col. 1, lines 6-43).

12. Claim 39 is rejected under 35 U.S.C. 103(a) as being unpatentable over Otsuki, U.S. Patent No. 5,751,805, in view of Dent, U.S. Patent No. 5,081,679. Referring to claim 39, Otsuki discloses a data protecting system wherein upon purchase of an encrypted software package a user requests his identifier and decryption key from the software house (Col. 4, lines 1-17), which meets the limitation of a transmitter configured to transmit a demand to said center unit for obtaining an encrypted data needed for decrypting said ciphered encryption algorithm. The software house distributes the random encryption key to the user encrypted with the identifier (Col. 4, lines 1-10), which meets the limitation of a key controller configured to renew said common cipher-key so as to be identical with said renewed common cipher-key in case of receiving said demand from said transmitter, and an encoder configured to produce said

Art Unit: 2132

encrypted data by encrypting a cipher-key with said renewed common cipher-key and to transmit said encrypted data to said terminal unit. Once the user receives the encrypted random encryption key the software installation module can prepare the loader to decrypt the software (Col. 4, lines 18-21). The encrypted random key is then decrypted using the identifier entered by the user. Once decrypted the random key is then used to decrypt an encrypted encryption algorithm that is stored on the user's IC card in order to decrypt the encrypted software (Col. 4, lines 34-46), which meets the limitation of an encryption controller configured to renew said common cipher-key in case of receiving said encrypted data from said center unit in response to said demand, and to produce an encryption algorithm by decrypting said encrypted data with the renewed common cipher-key. Otsuki does not disclose a counter being used during the rekeying process. Dent discloses a method of synchronizing encryption keys where encrypted communications are prevented when the counters at the terminals are offset (Col. 4, lines 43-68). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a counter in the rekeying method of Otsuki in order to ensure that communication is occurring with the proper terminal.

### ***Conclusion***

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after

Art Unit: 2132

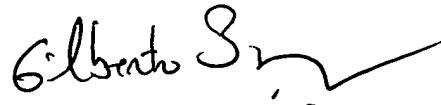
the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th0 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
Benjamin E. Lanier

  
GILBERTO BARRON JR.  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100